

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 The SUBJECT PREMISES, 24507 SE Mirrmont
 Blvd, Issaquah, WA, more fully described in
 Attachment A

Case No. MJ20-693

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The SUBJECT PREMISES, 24507 SE Mirrmont Blvd, Issaquah, WA, more fully described in Attachment A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

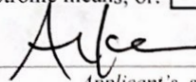
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C §§ 1014, 1343, and 1344	False Statements in Support of a Loan Application, Wire Fraud, and Bank Fraud

The application is based on these facts:

☒ See Affidavit of Special Agent Alan Keene, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.




Applicant's signature

Alan Keene, TIGTA Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/26/2020



Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or other have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to determine probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code Sections 1014 (False Statements in Support of a Loan Application), 1343 (Wire Fraud) and 1344 (Bank Fraud) will be found on the SUBJECT PREMISES.

THE INVESTIGATION

The Paycheck Protection Program ("PPP")

5. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act is a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of up to \$349 billion in forgivable loans to small businesses for job retention and certain other expenses, through a program referred to as the PPP. In or around April 2020, Congress authorized over \$300 billion in additional PPP funding.

6. In order to obtain a PPP loan, a qualifying business must submit a PPP loan application, which is signed by an authorized representative of the business. The PPP loan application requires the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications in order to be eligible to obtain the PPP loan. In the PPP loan application, the small business (through its authorized representative) must state, among other things, its: (a) average monthly payroll expenses; and (b) number of employees. These figures are used to calculate the amount of money the small business is eligible to receive under the PPP. In addition, businesses applying for a PPP loan must provide documentation showing their payroll expenses.

7. A PPP loan application must be processed by a participating financial institution (the lender). If a PPP loan application is approved, the participating financial institution funds the PPP loan using its own monies, which are 100% guaranteed by Small

1 Business Administration (SBA). Data from the application, including information about
 2 the borrower, the total amount of the loan, and the listed number of employees, is
 3 transmitted by the lender to the SBA in the course of processing the loan.

4 8. PPP loan proceeds must be used by the business on certain permissible
 5 expenses—payroll costs, interest on mortgages, rent, and utilities. The PPP allows the
 6 interest and principal on the PPP loan to be entirely forgiven if the business spends the loan
 7 proceeds on these expense items within a designated period of time and uses a certain
 8 percentage of the PPP loan proceeds on payroll expenses.

9 *The Economic Injury Disaster Relief Program (“EIDL”)*

10 9. The EIDL program is an SBA program that provides low-interest financing
 11 to small businesses, renters, and homeowners in regions affected by declared disasters.

12 10. The CARES Act authorized the SBA to provide EIDLs of up to \$2 million
 13 to eligible small businesses experiencing substantial financial disruption due to the
 14 COVID-19 pandemic. In addition, the CARES Act authorized the SBA to issue advances
 15 of up to \$10,000 to small businesses within three days of applying for an EIDL. The
 16 amount of the advance is determined by the number of employees the applicant certifies
 17 having. The advances do not have to be repaid.

18 11. In order to obtain an EIDL and advance, a qualifying business must submit
 19 an application to the SBA and provide information about its operations, such as the number
 20 of employees, gross revenues for the 12-month period preceding the disaster, and cost of
 21 goods sold in the 12-month period preceding the disaster. In the case of EIDLs for COVID-
 22 19 relief, the 12-month period was that preceding January 31, 2020. The applicant must
 23 also certify that all of the information in the application is true and correct to the best of
 24 the applicant’s knowledge.

25 12. EIDL applications are submitted directly to the SBA and processed by the
 26 agency with support from a government contractor. The amount of the loan, if the
 27 application is approved, is determined based, in part, on the information provided by the
 28 application about employment, revenue, and cost of goods, as described above. Any funds

1 issued under an EIDL or advance are issued directly by the SBA. EIDL funds can be used
 2 for payroll expenses, sick leave, production costs, and business obligations, such as debts,
 3 rent, and mortgage payments. If the applicant also obtains a loan under the PPP, the EIDL
 4 funds cannot be used for the same purpose as the PPP funds.

5 *The Defendant and Other Relevant Individuals and Entities*

6 13. AUSTIN HSU is a United States citizen residing at the SUBJECT
 7 PREMISES.

8 14. Chaoying Zhou (aka “Jill Ato”) is a United States citizen who resides with
 9 HSU at the SUBJECT PREMISES.

10 15. Blackrock Services P.S. (d/b/a “Back 2 Health Bellevue”) (“Blackrock”) is
 11 a Washington professional service corporation with offices in Bellevue, Washington.
 12 Blackrock offers chiropractic treatment and rehabilitation care. HSU is Blackrock’s owner
 13 and CEO. Zhou is Blackrock’s Managing Director.

14 16. Evergreen was a Washington corporation first registered on or about
 15 December 12, 2013.

16 17. Huggtopus was a Washington corporation first registered on or about June
 17 17, 2014.

18 18. Prodigy was a Washington corporation first registered on or about July 13,
 19 2018.

20 19. Sequoia was a Washington corporation first registered on or about May 8,
 21 2018.

22 20. Blueline was a Wyoming corporation first registered on or about June 26,
 23 2020.

24 *Overview of the Fraud*

25 21. As described further below, evidence gathered in the investigation
 26 demonstrates that, from in or around April 2020 through in or around August 2020, HSU
 27 submitted, or caused to be submitted, fraudulent loan applications to approved lenders and
 28 the SBA in order to obtain funds through the PPP and EIDL program. Among other things,

HSU fraudulently used the names of current and former Blackrock employees to obtain PPP loans on behalf of Evergreen, Huggtopus, Prodigy, and Sequoia.¹ HSU misrepresented that these current and former Blackrock employees had also worked for and been paid by these other companies, when, in truth, they had not.

22. In connection with this fraud, HSU submitted, or caused to be submitted, the following fraudulent loan applications:

Applicant	Amount Sought	Lender	Approx. Date of Application	Status
Sequoia	\$54,627.97	Celtic Bank Corporation ("Celtic")	4/27/2020	Approved
Prodigy	\$105,451	Kabbage, Inc. ("Kabbage")	5/7/2020	Approved
Evergreen	\$133,275	Kabbage	5/10/2020	Approved
Huggtopus	\$115,751	Kabbage	5/13/2020	Approved
Evergreen	\$150,000	SBA	3/29/2020	Approved
Huggtopus	\$150,000	SBA	5/17/2020	Canceled
Huggtopus	\$150,000	SBA	7/12/2020	Canceled
Sequoia	\$150,000	SBA	7/12/2020	Canceled
Blueline	\$150,000	SBA	7/12/2020	Approved
TOTAL:	\$1,159,104.97			

23. HSU distributed fraudulently obtained PPP loan proceeds to himself and Zhou.

Fraudulent PPP Loan Application Submitted on Behalf of Sequoia

24. According to records obtained from Celtic, on or about April 27, 2020,

¹ In March and April 2020, HSU had applied for a total of \$219,100 from EIDL and PPP loan proceeds on behalf of Blackrock.

1 HSU applied to Celtic for a PPP loan on behalf of Sequoia in the amount of \$54,627.97 via
2 Square's online application portal.

3 25. In the application, HSU represented that Sequoia had 12 employees.

4 26. Based on records obtained from Celtic and Square, HSU submitted several
5 documents in support of Blackrock's PPP loan application, including:

6 a. Internal Revenue Service ("IRS") Form 940, in which HSU represented
7 that Sequoia had made \$242,182.22 in total payments to Sequoia's
8 employees in 2019. HSU further represented that Sequoia had deposited
\$12,850.92 in federal unemployment taxes in 2019.

9 b. An IRS Form 941, in which HSU represented that Sequoia had paid its
10 employees tips, wages and other compensation for January, February and
11 March 2020 totaling \$95,115.65. HSU further represented that Sequoia
12 had deposited \$23,565.82 in federal unemployment taxes for the first
quarter of 2020.

13 c. A copy of HSU's driver license.

14 27. The Sequoia PPP application represented that the business employed 12
15 employees. Evidence gathered in the government's investigation demonstrates that this
16 statement is false:

17 a. Information obtained from the Washington State Employment Security
18 Department ("ESD") shows the agency has no record of any employees
being employed by Sequoia.

19 b. Information obtained from the Social Security Administration ("SSA")
20 revealed that Sequoia did not file any Forms W-2 or W-3 for any
21 employees for 2019.

22 c. Payroll records obtained from Intuit, a payroll processor, show Sequoia
23 did not make any payroll payments in 2019 or in the first quarter of 2020.

24 d. Information obtained from the Washington State Department of Revenue
25 ("DoR") revealed that Sequoia had not registered with DoR or applied for
a business license.

26 28. The IRS Forms 940 and 941 submitted with the Sequoia PPP application
27 also appear to be fraudulent. Records from the IRS confirm that these returns had not been
28 filed with the IRS and the amounts of tax deposits reported on the Forms 940 and 941 were
not paid to the IRS. In fact, Sequoia had not filed employment tax or federal income tax

1 returns with the IRS in 2019 or 2020, and had not made employment tax deposits in 2019
2 or 2020.

3 29. According to records obtained from Celtic, it approved Sequoia's PPP
4 application and funded the loan. According to records obtained from Bank of America, on
5 or about May 4, 2020, Celtic transferred \$54,627.97 to a bank account in the name of
6 Blackrock at Bank of America, for which HSU was the sole signatory.

7 *Fraudulent PPP Loan Application Submitted on Behalf of Prodigy*

8 30. According to records obtained from Kabbage, on or about May 7, 2020,
9 Kabbage received a PPP application in the name of Prodigy seeking a PPP loan in the
10 amount of \$105,451. The application was submitted in the name of Zhou², who was
11 represented to be Prodigy's majority owner.

12 31. In the Prodigy PPP application, an individual purporting to be Zhou
13 represented that Prodigy had 14 employees and that its average monthly payroll was
14 \$42,181.

15 32. In the Prodigy PPP application, an individual purporting to be Zhou made
16 several certifications, including that Prodigy "was in operation on February 15, 2020 and
17 had employees for whom it paid salaries and payroll taxes or paid independent
18 contractors."

19 33. Based on records obtained from Kabbage, several documents were
20 submitted in support of Prodigy's PPP loan application, including: (a) a Form 940, which
21 represented that Prodigy had made \$506,169.11 in total payments to Prodigy's employees
22 in 2019; (b) Forms W-2 and W-3 for 21 individuals who were purportedly employed by
23 Prodigy in 2019; and (c) a copy of Zhou's driver license.

24
25
26
27 ² On or about October 7, 2020, a recorded call was made to Zhou by an investigator posing as an employee of the
28 SBA. The investigator made the call to Phone Number 1, which was the same phone number listed on an EIDL
application in the name of Prodigy. On the recorded call, Zhou stated that she had not filed Prodigy's PPP application
herself, but that HSU had filed it for her.

34. The government's investigation has revealed that Prodigy's application to Kabbage contained materially false and misleading information.

- a. In or around September and October 2020, law enforcement interviewed three individuals listed as purported Prodigy employees. All three employees confirmed they had never been paid by Prodigy; rather, they were all paid employees of BlackRock (which received its own separate PPP loan).³
- b. Further investigation revealed that all of the names listed as employees on the Prodigy PPP application were also used in the fake Evergreen and Huggtopus Forms W-2 and W-3 (described below). In many cases, the reported wages and withholdings for these individuals were identical or nearly identical across the three companies.
- c. Additionally, information obtained from the IRS further revealed that Prodigy's Employer Identification Number ("EIN") had only been created on April 27, 2020 (*i.e.*, two weeks before Prodigy's PPP loan application was submitted), and that in the EIN application, which listed HSU as the responsible party and was filed from an IP address registered to the SUBJECT PREMISES, HSU represented that Prodigy would not have any employees during the following 12-month period.
- d. Information obtained from the SSA revealed that Prodigy did not file any Forms W-2 or W-3 for any employees for 2019.

35. According to records obtained from Kabbage, it approved Prodigy's application and funded the loan. According to records obtained from Bank of America, on or about May 11, 2020, Kabbage transferred \$105,451 to Prodigy's bank account at Bank of America, for which HSU was the sole signatory.

Fraudulent PPP Loan Application Submitted on Behalf of Evergreen

36. According to records obtained from Kabbage, on or about May 10, 2020, Kabbage received a PPP application in the name of Evergreen seeking a PPP loan in the amount of \$133,275⁴. The application was submitted in the name of HSU, who was represented to be Evergreen's sole owner and CEO.

³ These individuals, who were also listed as Evergreen and Huggtopus employees, also confirmed they had never been paid by these companies; rather, they were all paid employees of BlackRock.

⁴ According to records obtained from Kabbage and information from the SBA, the original lender listed on the loan note was Cross River Bank. The loan was subsequently serviced by Kabbage.

37. The application represented that Evergreen had 13 employees and that its average monthly payroll was \$53,310. Several documents were submitted in support of Evergreen's PPP loan application, including Forms W-2 and W-3 for 22 individuals who were purportedly employed by Evergreen in 2019.

38. The government's investigation has revealed that Evergreen's application to Kabbage contained materially false and misleading information.

- a. Nearly all of the names listed as employees of Evergreen were also listed in the fake Prodigy and Huggtopus Forms W-2 and W-3 described above and below and, in many cases, the reported wages and withholdings for these individuals were identical or nearly identical across the three companies. Information obtained from the SSA revealed that Evergreen did not file any Forms W-2 or W-3 for any employees for 2019.
- b. Information obtained from the IRS revealed that Evergreen had not filed employment tax or federal income tax returns in 2019 or 2020, nor did Evergreen make employment tax deposits during 2019 or 2020. In fact, HSU had only applied for an EIN for Evergreen on May 6, 2020 (*i.e.*, four days before HSU submitted Evergreen's PPP loan application).
- c. Information obtained from the ESD shows the agency has no record of any employees being employed by Evergreen.
- d. Information obtained from the DoR revealed that when, on June 1, 2020, Evergreen applied to renew its business license, HSU indicated Evergreen had only 3 employees (not 13). HSU also listed Evergreen's annual gross income as between \$0 and \$12,000.

39. According to records obtained from Kabbage, it approved Evergreen's application and funded the loan. According to records obtained from Bank of America, on or about May 12, 2020, Lender 3 transferred \$133,275 to Sequoia's bank account at Bank of America, for which HSU was the sole signatory.

Fraudulent PPP Loan Application Submitted on Behalf of Huggtopus

40. According to records obtained from Kabbage, on or about May 13, 2020, Kabbage received a PPP application in the name of Huggtopus seeking a PPP loan in the amount of \$115,751. The application was submitted in the name of HSU, who was represented to be one of Huggtopus's owners and its Managing Partner.

41. In the application, HSU represented that Huggtopus had 12 employees and that its average monthly payroll was \$46,301. Several documents were submitted in support of Huggtopus's PPP loan application, including: (a) Forms W-2 and W-3 for 21 individuals who were purportedly employed by Huggtopus in 2019 and (b) a copy of HSU's driver license.

42. The government's investigation has revealed that Huggtopus's application to Kabbage contained materially false and misleading information.

- a. All of the names listed as employees of Huggtopus were also listed in the fake Prodigy and Evergreen Forms W-2 and W-3 described above and, in many cases, the reported wages and withholdings for these individuals were identical or nearly identical across the three companies. Information obtained from the SSA revealed that Huggtopus did not file any Forms W-2 or W-3 for any employees for 2019.
- b. Information obtained from the ESD shows the agency has no record of any employees being employed by Huggtopus.
- c. Information obtained from the IRS revealed that Huggtopus had not filed any employment tax or federal income tax returns with the IRS in 2019 or 2020, nor did Huggtopus make any employment tax deposits during 2019 or 2020.
- d. Payroll records obtained from Intuit show Huggtopus did not make any payroll payments in 2019 or in the first quarter of 2020.
- e. Information obtained from the DoR revealed that Huggtopus's business license had been administratively revoked on June 30, 2019.

Fraudulent EIDL Loan Application Submitted on Behalf of Evergreen

43. According to records obtained from the SBA, on or about March 29, 2020, the SBA received an application in the name of Evergreen seeking an EIDL loan in the amount of \$150,000. The application was submitted in the name of HSU via the SBA's online portal.

44. HSU falsely certified Evergreen "is not engaged in any activity that is illegal under federal, state, or local law." Records obtained from the Washington State Liquor and Cannabis Board revealed that Evergreen is operated as a recreational marijuana

1 producer. The manufacture of a controlled substance, such as marijuana, is illegal under
 2 federal law Title 18, United States Code, Section 841, Manufacture of a Controlled
 3 Substance.

4 45. The SBA approved Evergreen's application and funded the loan. On or
 5 about June 29, 2020, the SBA wired \$149,900 to Evergreen's Umpqua bank account, for
 6 which HSU is the sole signatory.

7 *Fraudulent EIDL Loan Applications Submitted on Behalf of Huggtopus*

8 46. According to records obtained from the SBA, on or about May 17, 2020,
 9 the SBA received an application in the name of Huggtopus seeking an EIDL loan in the
 10 amount of \$150,000. On or about July 12, 2020, the SBA received a second application in
 11 the name of Huggtopus seeking an EIDL loan in the same amount. Both applications were
 12 submitted in the name of HSU via the SBA's online portal.

13 47. These applications contained conflicting information:

- 14 a. In the first application, HSU represented that Huggtopus was in the
 15 agriculture industry, and that, in the 12 months prior to the disaster,
 16 Huggtopus had 13 employees, gross receipts of \$1,218,092, and cost of
 goods sold of \$324,901.
- 17 b. In the second application, HSU represented that Huggtopus was in the
 18 health care services industry, and that, in the 12 months prior to the
 19 disaster, Huggtopus had 9 employees, gross receipts of \$1,490,230 and
 cost of goods sold of \$340,290.

20 48. As described above in paragraph 42, evidence gathered in the government's
 21 investigation demonstrates that these statements about the number of employees are false.

22 49. The SBA denied Huggtopus's fraudulent applications as duplicative.

23 *Fraudulent EIDL Loan Application Submitted on Behalf of Sequoia*

24 50. According to records obtained from the SBA, on or about July 12, 2020,
 25 the SBA received an application in the name of Sequoia seeking an EIDL loan in the
 26 amount of \$150,000. The application was submitted in the name of HSU via the SBA's
 27 online portal.

1 51. In the application, HSU represented that Sequoia had 12 employees. As
 2 described above in paragraph 27, evidence gathered in the government's investigation
 3 demonstrates that this statement is false.

4 52. The SBA denied Sequoia's fraudulent application as duplicative.

5 *Fraudulent EIDL Loan Application Submitted on Behalf of Blueline*

6 53. According to records obtained from the SBA, on or about July 12, 2020,
 7 the SBA received an application in the name of Blueline seeking an EIDL loan in the
 8 amount of \$150,000. The application was submitted in the name of HSU, who was
 9 represented to be Blueline's sole owner and Chief Financial Officer. HSU submitted the
 10 application via the SBA's online portal.

11 54. In the application, HSU represented that Blueline was established on April
 12 3, 2017 and that he has owned Blueline since that time. HSU also represented that Blueline
 13 had 9 employees.

14 55. The SBA approved Blueline's application and funded the loan. On or about
 15 August 3, 2020, the SBA sent \$149,900 via an interstate wire from the SBA's bank account
 16 in Denver, Colorado to HSU's Salal Credit Union bank account in Seattle, Washington, for
 17 which he is the sole signatory.

18 56. The government's investigation has revealed that Blueline's application to
 19 the SBA contained materially false and misleading statements.

20 57. HSU's representation that Blueline was established on April 3, 2017 and
 21 that HSU has owned Blueline since that time is false:

- 22 a. According to records obtained from the Wyoming Secretary of State and
 23 Cloud Peak Law, LLC, Blueline was formed on June 26, 2020 at HSU's
 24 request.
- 25 b. IRS records show that the EIN for Blueline was created on or about June
 26 29, 2020 using personal information belonging to Betty Hsu, HSU's
 27 mother.
- 28 c. On October 13, 2020, law enforcement interviewed Betty Hsu and Betty
 Hsu confirmed that she entered into an agreement with HSU to form
 Blueline to sell facemasks beginning in August 2020.

1 58. HSU's representations that, during prior 12 months leading to the disaster,
 2 Blueline had 9 employees, \$1,509,920 in gross receipts and \$628,990 in cost of goods sold,
 3 are false:

- 4 a. IRS records show that the EIN for Blueline was created on or about June
 5 29, 2020 using Betty Hsu's personal information.
- 6 b. On October 13, 2020, Betty Hsu was interviewed and confirmed that
 7 Blueline did not have any employees or sales.
- 8 c. Information obtained from the DoR revealed that Blueline had not
 9 registered with DoR or applied for a business license.

10 *Probable Cause that Evidence of Crimes Will be Found at SUBJECT PREMISES*

11 59. There is probable cause that evidence, fruits and instrumentalities of the
 12 crime under investigation will be found at the SUBJECT PREMISES. Based upon HSU's
 13 driver's license, records obtained from Bank of America, Kabbage, Celtic, and the WA
 14 LCB, HSU resides at the SUBJECT PREMISES, which is a residential home. Moreover,
 15 HSU listed the SUBJECT PREMISES as his business address on the PPP loan applications
 16 for the Evergreen and Sequoia PPP loans and the Evergreen EIDL loan. HSU listed his
 17 individual contact address as the SUBJECT PREMISES on the EIDL loan applications for
 18 Evergreen, Huggtopus, Sequoia, and Blueline. HSU also listed his residential address as
 19 the SUBJECT PREMISES on PPP loan applications submitted to Kabbage and Celtic for
 20 Sequoia, Evergreen, and Huggtopus.

21 60. There is probable cause that HSU used computers, the Internet, and other
 22 digital devices, such as a mobile telephone, as instrumentalities of, and as storage devices
 23 with respect to the crimes under investigation:

- 24 a. Based on records obtained from Celtic and Square, HSU submitted the PPP
 25 loan application for Sequoia via Square's website using the Internet.
- 26 b. Based on records obtained from Kabbage, HSU logged into Kabbage's
 27 online system to process the PPP loans and to uploaded documents such as
 28 the Forms W-2, W-3 and his or Zhou's driver's license submitted with the
 Evergreen, Huggtopus, and Prodigy PPP loans. Kabbage records showed
 that from on or about May 6, 2020 through May 13, 2020, HSU logged into
 Kabbage's online system using an IP address serviced by Comcast. Comcast

records obtained during the investigation revealed that the IP addresses on the dates that documents were uploaded was associated to a Comcast account under Zhou's name with a service address listed as the SUBJECT PREMISES.

- c. Based on records obtained from Kabbage, HSU submitted Forms W-2s, W-3, and worksheets with the PPP loans for Prodigy, Huggtopus, and Evergreen. Based upon my training and experience, there is probable cause to believe that these documents were created using a computer or other digital device. On each set of W-2 worksheets submitted with the three loans, the bottom of the worksheet is annotated with the phrase "QBDT" and a date. From my knowledge and experience, QBDT is an acronym for QuickBooks Desktop, which is a computer application that can be used to process payroll amongst other features.
- d. Based on information obtained from the IRS, Prodigy's EIN application, which listed HSU as the responsible party, was filed on April 27, 2020 from an IP address registered to the SUBJECT PREMISES.
- e. Based on records from Kabbage and Square, HSU received automated emails regarding the processing of the PPP loans for Evergreen, Huggtopus, Sequoia, and Prodigy. For example, on or about May 12, 2020 HSU, via the email address on the application, jackielee219@yahoo.com, received an automated email from Kabbage indicating that the \$115,751 PPP loan for Huggtopus was approved. The email advised HSU to sign in to Kabbage to complete the loan process. In my training and experience, HSU would have had to use a computer or other digital device with an Internet connection (such as a smart phone), to receive these emails.
- f. Based on records obtained from the SBA, HSU used an online SBA system, to apply for EIDL loans for Evergreen, Blueline, Huggtopus, and Sequoia.

61. There is probable cause that the computers and digital devices that HSU used as instrumentalities of, and as storage devices with respect to, the crimes under investigation are located at the SUBJECT PREMISES. Based on records obtained from Comcast, digital devices used by HSU in furtherance of the fraudulent scheme used IP addresses traceable back to the SUBJECT PREMISES. For example:

- a. IP address 71.197.162.198 was assigned to Zhou at the SUBJECT PREMISES from April 27, 2020 through April 30, 2020. Based on records obtained from Square and Celtic, a digital device used this IP address during that period to log into Square during the processing of the Sequoia PPP loan.

- b. IP address 2601:600:9780:24db:64b7:f6d6:e916:cd2 was assigned to Zhou at the SUBJECT PREMISES from April 27, 2020. Based on records obtained from the IRS, a digital device used this IP address on that date to log into IRS online portal and obtained an EIN for Prodigy. The EIN was subsequently used to apply for and obtain the PPP loan for Prodigy.
- c. IP address 71.197.162.198 was assigned to Zhou at the SUBJECT PREMISES from May 6, 2020 through May 13, 2020. Based on records obtained from Kabbage, a digital device used this IP address during that time period to log into Kabbage during the processing of the PPP loans for Evergreen, Huggtopus, and Prodigy.
- d. IP address 2601:600:9780:24db:3535:345:a904:42bd was assigned to Zhou at the SUBJECT PREMISES on July 12, 2020. Based on records obtained from the SBA, a digital device used this IP address on that date was used to submit the EIDL application for BlueLine.

TECHNICAL TERMS

62. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every digital device attached to the Internet must be assigned an **IP** address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of **IP** addresses. Some computers have static-that is, long-term IP addresses, while other computers have dynamic-that is, frequently-changed IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Electronic Storage media: Electronic Storage media is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, and FORENSIC ANALYSIS

63. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices⁵ such as computer hard drives or other electronic storage media⁶. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

64. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the crimes of making false statements in support of a loan application (18 U.S.C. § 1014), wire fraud (18 U.S.C. § 1343), and bank fraud (18 U.S.C. § 1344), will be stored on those digital devices or other electronic storage media. I believe digital devices or other electronic storage media are being used to: (i) create the fraudulent PPP loan applications and supporting documents, including fake federal tax filings and fake W-2s and W-3; (ii) send and receive emails with lenders and Zhou about the fraudulent PPP loan applications; (iii) create fraudulent EIDL loan applications; (iv) open and access online bank accounts, including the bank accounts into which the proceeds of the fraud were deposited. There is, therefore, probable cause to

⁵ “Digital device” includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (“GPS”), or portable media players.

⁶ Electronic Storage media is any physical object upon which electronically stored information can be recorded.

Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 believe that evidence, fruits and/or instrumentalities of the crimes of making false
 2 statements in support of a loan application (18 U.S.C. § 1014), wire fraud (18 U.S.C. §
 3 1343), and bank fraud (18 U.S.C. § 1344), exists and will be found on digital device or
 4 other electronic storage media at the SUBJECT PREMISES, for at least the following
 5 reasons:

- 6 a. Based on my knowledge, training, and experience, I know that computer files
 7 or remnants of such files can be preserved (and consequently also then
 8 recovered) for months or even years after they have been downloaded onto a
 9 storage medium, deleted, or accessed or viewed via the Internet. Electronic
 10 files downloaded to a digital device or other electronic storage medium can
 11 be stored for years at little or no cost. Even when files have been deleted,
 12 they can be recovered months or years later using forensic tools. This is so
 13 because when a person “deletes” a file on a digital device or other electronic
 14 storage media, the data contained in the file does not actually disappear;
 15 rather, that data remains on the storage medium until it is overwritten by new
 16 data.
- 17 b. Therefore, deleted files, or remnants of deleted files, may reside in free space
 18 or slack space—that is, in space on the digital device or other electronic
 19 storage medium that is not currently being used by an active file for long
 20 periods of time before they are overwritten. In addition, a computer's
 21 operating system may also keep a record of deleted data in a “swap” or
 22 “recovery” file.
- 23 c. Wholly apart from user-generated files, computer storage media—in
 24 particular, computers' internal hard drives—contain electronic evidence of
 25 how a computer has been used, what it has been used for, and who has used
 26 it. To give a few examples, this forensic evidence can take the form of
 27 operating system configurations, artifacts from operating system or
 28 application operation; file system data structures, and virtual memory “swap”
 or paging files. Computer users typically do not erase or delete this evidence,
 because special software is typically required for that task. However, it is
 technically possible to delete this information.

Similarly, files that have been viewed via the Internet are sometimes
 automatically downloaded into a temporary Internet directory or “cache.”

65. Based on actual inspection of PPP loan applications, payroll reports,
 Forms 940 and 941, Forms W-2, W-3 and Worksheets, and related email correspondence,
 I am aware that digital devices and other electronic storage media were used to generate,

1 store, and electronically send documents used in the fraudulent scheme. There is reason
 2 to believe that there is a computer and other digital devices currently located at the
 3 SUBJECT PREMISES.

4 66. *Forensic evidence.* As further described in Attachment B, this application
 5 seeks permission to locate not only computer files that might serve as direct evidence of
 6 the crimes described on the warrant, but also for forensic electronic evidence that
 7 establishes how digital devices or other electronic storage media were used, the purpose
 8 of their use, who used them, and when. There is probable cause to believe that this
 9 forensic electronic evidence will be on any digital devices or other electronic storage
 10 media located at the SUBJECT PREMISES because:

- 11 a. Stored data can provide evidence of a file that was once on the digital device
 12 or other electronic storage media but has since been deleted or edited, or of
 13 a deleted portion of a file (such as a paragraph that has been deleted from a
 14 word processing file). Virtual memory paging systems can leave traces of
 15 information on the digital device or other electronic storage media that show
 16 what tasks and processes were recently active. Web browsers, e-mail
 17 programs, and chat programs store configuration information that can reveal
 18 information such as online nicknames and passwords. Operating systems can
 19 record additional information, such as the history of connections to other
 20 computers, the attachment of peripherals, the attachment of USB flash
 storage devices or other external storage media, and the times the digital
 device or other electronic storage media was in use. Computer file systems
 can record information about the dates files were created and the sequence in
 which they were created.
- 21 b. As explained herein, information stored within a computer and other
 22 electronic storage media may provide crucial evidence of the "who, what,
 23 why, when, where, and how" of the criminal conduct under investigation,
 24 thus enabling the United States to establish and prove each element or
 25 alternatively, to exclude the innocent from further suspicion. In my training
 26 and experience, information stored within a computer or storage media (e.g.,
 27 registry information, communications, images and movies, transactional
 28 information, records of session times and durations, internet history, and anti-
 virus, spyware, and malware detection programs) can indicate who has used
 or controlled the computer or storage media. This "user attribution" evidence
 is analogous to the search for "indicia of occupancy" while executing a search
 warrant at a residence. The existence or absence of anti-virus, spyware, and
 malware detection programs may indicate whether the computer was

remotely accessed, thus inculcating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation⁷. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic

⁷ For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an Internet browser to log into a bank account in the name of John Doe; b) at 11:02am the Internet browser was used to download child pornography; and c) at 11:05 am the Internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIME

67. As explained above in paragraphs 60 through and including 61, I believe computers, digital devices or other electronic storage media are being used to: (i) create the fraudulent PPP loan applications and supporting documents, including fake federal tax filings and fake W2s; (ii) send and receive emails with lenders and Zhou about the fraudulent PPP loan applications; (iii) create fraudulent EIDL loan applications; and (iv) open and access online bank accounts, including bank accounts in which the proceeds of the fraud were deposited.

PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION

68. I have not made any prior efforts to obtain evidence from HSU's digital devices, including his mobile telephone, based on HSU's consent. I believe, based upon the nature of the investigation and the information I have received, that if HSU becomes aware of the investigation in advance of the execution of a search warrant, he may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation. Further, documents obtained during the investigation showed that HSU appeared uncooperative or non-responsive with state agencies conducting civil inquiries such as the WA Department of Revenue and WA Employment Security Department.

**REQUEST FOR AUTHORITY TO
CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS**

69. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

- 1 c. *Variety of forms of electronic media.* Records sought under this warrant
 2 could be stored in a variety of electronic storage media formats and on a
 3 variety of digital devices that may require off-site reviewing with
 4 specialized forensic tools.

5 SEARCH TECHNIQUES

6 70. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
 7 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,
 8 or otherwise copying digital devices or other electronic storage media that reasonably
 9 appear capable of containing some or all of the data or items that fall within the scope of
 10 Attachment B to this Affidavit, and will specifically authorize a later review of the media
 11 or information consistent with the warrant.

12 71. Because at least two people share the SUBJECT PREMISES as a
 13 residence, including HSU's partner, Chaoying Zhou (aka "Jill Ato"), it is possible that
 14 the SUBJECT PREMISES will contain digital devices or other electronic storage
 15 media that are predominantly used, and perhaps owned, by persons who are not
 16 suspected of a crime. If agents conducting the search nonetheless determine that it is
 17 possible that the things described in this warrant could be found on those computers,
 18 this application seeks permission to search and if necessary to seize those computers
 19 as well. It may be impossible to determine, on scene, which computers.

20 72. Consistent with the above, I hereby request the Court's permission to seize
 21 and/or obtain a forensic image of digital devices or other electronic storage media that
 22 reasonably appear capable of containing data or items that fall within the scope of
 23 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or
 24 other electronic storage media and/or forensic images, using the following procedures:

25 **A. Processing the Search Sites and Securing the Data.**

- 26 a. Upon securing the physical search site, the search team will conduct an
 27 initial review of any digital devices or other electronic storage media
 28 located at the subject premises described in Attachment A that are capable
 of containing data or items that fall within the scope of Attachment B to
 this Affidavit, to determine if it is possible to secure the data contained on

these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

- b. In order to examine the electronically stored information (“ESP”) in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit⁸.
- c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.
- d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

⁸ The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

B. Searching the Forensic Image

- a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

**REQUEST FOR AUTHORITY TO USE HSU'S BIOMETRIC FEATURES TO
UNLOCK DEVICES WHERE NECESSARY**

73. The warrant requests the ability for law enforcement agents to obtain from the person of HSU (but not any other individuals who may be present at the SUBJECT PREMISES at the time of execution of the warrant), the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial, including iris, characteristics), necessary to unlock any digital devices subject to seizure pursuant to the warrant and requiring such biometric access for which law enforcement has reasonable suspicion to believe that HSU's physical biometric characteristics will unlock the devices. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many digital devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features.

- 1 b. Some devices offer a combination of these biometric features, and the user
2 of such devices can select which features they would like to utilize.
- 3 c. If a device is equipped with a fingerprint scanner, a user may enable the
4 ability to unlock the device through his or her fingerprints. For example,
5 Apple offers a feature called "Touch ID," which allows a user to register up
6 to five fingerprints that can unlock a device. Once a fingerprint is registered,
7 a user can unlock the device by pressing the relevant finger to the device's
8 Touch ID sensor, which is found in the round button (often referred to as the
9 "home" button) located at the bottom center of the front of the device. The
10 fingerprint sensors found on devices produced by other manufacturers have
11 different names but operate similarly to Touch **ID**.
- 12 d. If a device is equipped with a facial-recognition feature, a user may enable
13 the ability to unlock the device through his or her face. For example, this
14 feature is available on certain Android devices and is called "Trusted Face."
15 During the Trusted Face registration process, the user holds the device in
16 front of his or her face. The device's front-facing camera then analyzes and
17 records data based on the user's facial characteristics. The device can then
18 be unlocked if the front-facing camera detects a face with characteristics that
19 match those of the registered face. Facial recognition features found on
20 devices produced by other manufacturers (such as Apple's "Face ID") have
21 different names but operate similarly to Trusted Face.
- 22 e. If a device is equipped with an iris-recognition feature, a user may enable
23 the ability to unlock the device with his or her irises. For example, on
24 certain Microsoft devices, this feature is called "Windows Hello." During
25 the Windows Hello registration, a user registers his or her irises by
26 holding the device in front of his or her face. The device then directs an
27 infrared light toward the user's face and activates an infrared-sensitive
28 camera to record data based on patterns within the user's irises. The
device can then be unlocked if the infrared-sensitive camera detects the
registered irises. Iris-recognition features found on devices produced by
other manufacturers have different names but operate similarly to
Windows Hello.
- f. In my training and experience, users of electronic devices often enable the
aforementioned biometric features because they are considered to be a more
convenient way to unlock a device than by entering a numeric or
alphanumeric passcode or password. Moreover, in some instances,
biometric features are considered to be a more secure way to protect a
device's contents. This is particularly true when the users of a device are

engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

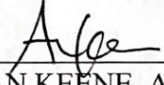
- g. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. Any passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- h. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- i. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to the warrant and may be unlocked using one of the aforementioned biometric features, the warrant permits law enforcement personnel to obtain from HSU the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices, including to (1) press or swipe HSU's fingers (including thumbs) to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of HSU's face to activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of HSU's face to activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by the warrant.

1 j. The proposed warrant does not authorize law enforcement to require that
2 HSU state or otherwise provide the password or identify which specific
3 biometric characteristics (including the unique finger(s) or other physical
4 features) may be used to unlock or access the devices. Nor does the
5 proposed warrant authorize law enforcement to use the fact that the warrant
6 allows law enforcement to obtain the display of any biometric
7 characteristics to compel HSU to state or otherwise provide that above-
8 described information. However, the voluntary disclosure of such
9 information by HSU would be permitted under the proposed warrant. To
10 avoid confusion on that point, if agents in executing the warrant ask HSU
11 for the password to any devices, or to identify which specific biometric
12 characteristic (including the unique finger(s) or other physical features)
13 unlocks any devices, the agents will not state or otherwise imply that the
14 warrant requires HSU to provide such information, and will make clear
15 that providing any such information is voluntary and that HSU is free to
16 refuse the request.
17
18
19
20
21
22
23
24
25
26
27
28

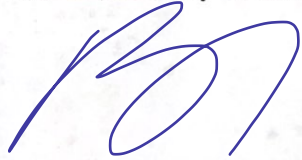
CONCLUSION

74. Based on the above facts, I respectfully submit that there is probable cause that evidence, fruits, and instrumentalities of violations of Title 18, United States Code Sections 1014 (False Statements in Support of a Loan Application), 1343 (Wire Fraud) and 1344 (Bank Fraud), are located at the SUBJECT PREMISES as more fully described in Attachment A to this Affidavit as well as on and in any digital devices or other electronic storage media found at the SUBJECT PREMISES. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES as well as any digital devices and electronic storage media located therein, including but not limited to a mobile telephone associated with the telephone number (206) 631-1906, for the items more fully described in Attachment B hereto incorporated herein by reference, and the seizure of any such items found therein.

75. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).


ALAN KEENE, Affiant
Special Agent, TIGTA

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit by telephone on this 26th day of October, 2020.


BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

ATTACHMENT A

The property to be searched is 24507 SE Mirrmont Blvd, Issaquah WA 98027, further described as a stand-alone two-story residence depicted in the photograph below (the “SUBJECT PREMISES”), and any digital devices or other electronic storage media found therein, including, but not limited to a mobile telephone associated with the telephone number (206) 631-1906. The SUBJECT PREMISES is accessible from the road via a driveway. To left of the driveway is a black mailbox with the number “24507” on a white sticker with black print.

FRONT (Agent Picture)



FRONT (FROM COUNTY ASSESSOR)



**ATTACHMENT B
ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium), that constitute evidence, instrumentalities, or fruits of violations of Title 18, United States Code Sections 1014 (False Statements in Support of a Loan Application), 1343 (Wire Fraud) and 1344 (Bank Fraud):

1. All documents for the period from January 2019 to the present relating to violations of Title 18, United States Code Sections 1014 (False Statements in Support of a Loan Application), 1343 (Wire Fraud) and 1344 (Bank Fraud), involving AUSTIN HSU of Chaoying Zhou (aka "Jill Ato"), including:

- a. All documents relating to Blackrock Services, Sequoia Corporation, Evergreen Inc., Evergreen LLC, Huggtopus Corporation, Prodigy Holdings PLLC., Blueline Capital LLC, or any affiliated entities or associated individuals;
- b. All documents relating to the Paycheck Protection Program ("PPP");
- c. All documents relating to PPP loan applications and supporting documentation;
- d. All documents relating to the Economic Impact Disaster Loan ("EIDL") program;
- e. All documents relating to EIDL loan applications and supporting documentation;

- f. All documents relating to the falsification of tax documents, Forms W-2 and W-3, bank records, incorporation documents, or other financial records;
 - g. All documents relating to the unauthorized use of a means of identification of a person or entity;
 - h. All documents relating to Bank of America, N.A., Salal Credit Union, Umpqua Bank, Square Inc., Square Capital, Cross River Bank, Kabbage Inc., and other financial statements and records related to HSU and his associated entities, and Chaoying Zhou and her associated entities.
 - i. All communications with any financial institution relating to PPP or EIDL loan proceeds;
 - j. All documents relating to the receipt, transfer, or other disposition of any criminal proceeds;
 - k. All banking and financial records, including, but not limited to, records reflecting the location and account information for bank accounts and brokerage or investment accounts associated with Blackrock Services, Sequoia Corporation, Evergreen Inc, Evergreen LLC, Hugstopus Corporation, Prodigy Holdings PLLC, AUSTIN HSU, Betty Hsu and/or Chaoying Zhou.
2. Digital devices¹ or other electronic storage media and/or their components, which include:
- a. Any digital device or other electronic storage media² capable of being used to commit, further, or store evidence of the offenses listed above;
 - b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

- c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
- d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;
- e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
- f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
- g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. Any digital devices or other electronic storage media that were or may have been used as a means to commit the offenses described on the warrant, including violations of Title 18, United States Code Sections 1014 (False Statements in Support of a Loan Application), 1343 (Wire Fraud) and 1344 (Bank Fraud).

4. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants; created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
- f. evidence of the times the digital device or other electronic storage media was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
- h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;
- i. contextual information necessary to understand the evidence described in this attachment.

5. If, during the execution of the search of described above in Attachment “B,” law enforcement personnel law encounter any devices that are subject to seizure pursuant to the warrant and for which law enforcement has reasonable suspicion to believe that AUSTIN HSU’s physical biometric characteristics will unlock the devices, this warrant permits law enforcement personnel to obtain from AUSTIN HSU the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the devices, including to (1) press or swipe AUSTIN HSU’s fingers (including thumbs) to the fingerprint scanner of the devices; (2) hold the devices found at the SUBJECT PREMISES in front of AUSTIN HSU's

1 face to activate the facial recognition feature; and/or (3) hold the devices found at the
2 SUBJECT PREMISES in front of AUSTIN HSU's face to activate the iris recognition
3 feature, for the purpose of attempting to unlock the devices in order to search the
4 contents as authorized by the warrant.
5

6 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
7 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
8 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
9 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
10 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
11 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
12 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
13 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
14 CRIMES.
15
16
17
18
19
20
21
22
23
24
25
26
27
28